CUAUHTEMOC ORTEGA (Bar No. 257443)
Federal Public Defender
GEORGINA WAKEFIELD (Bar No. 282094)
(E-Mail: Georgina_Wakefield@fd.org)
GABRIELA RIVERA (Bar No. 283633)
(E-Mail: Gabriela_Rivera@fd.org)
JULIA DEIXLER (Bar No. 301954)
(E-Mail: Julia_Deixler@fd.org)
Deputy Federal Public Defenders
321 East 2nd Street
Los Angeles, California 90012-4202
Telephone: (213) 894-2854
Facsimile: (213) 894-0081

Attorneys for Defendant
JERRY NEHL BOYLAN

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JERRY NEHL BOYLAN, Defendant.	Case No. 2:22-CR-00482-GW **DEFENDANT JERRY NEHL BOYLAN'S MOTION TO COMPEL GOVERNMENT TO PERMIT DEFENSE EXAMINATION OF DIGITAL DEVICES; EXCLUDING DATA FROM THE DEVICES AT TRIAL IN THE ALTERNATIVE**

Jerry Nehl Boylan, through his attorneys of record, Deputy Federal Public Defenders Georgina Wakefield, Gabriela Rivera, and Julia Deixler, hereby files defendant's motion to in the alternative to compel the government to permit a defense

/ / /

/ / /

/ / /

/ / /

/ / /

examination of the digital devices recovered from the wreckage of the Conception or to exclude any data from these devices at trial.

Respectfully submitted,

CUAUHTEMOC ORTEGA
Federal Public Defender

DATED: March 23, 2023

By */s/ Georgina Wakefield*
GEORGINA WAKEFIELD
GABRIELA RIVERA
JULIA DEIXLER
Deputy Federal Public Defenders
Attorneys for JERRY NEHL BOYLAN

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Federal Cases

TABLE OF AUTHORITIES

Page(s)

Other Authorities

I. INTRODUCTION

During its years-long investigation and prosecution of the instant case, the government seized and forensically searched several digital devices, including cell phones, computers, and hard drives. The government then made copies of each device, and its case agents conducted forensic searches of those copies. The government intends to introduce data from these devices during its case-in-chief. Yet the government has produced to the defense only limited items that its agents have identified as relevant to the prosecution. The defense has requested to inspect the complete copies of the digital devices, which the government has in its possession, custody, or control, but the government has declined all such defense requests. *See* Exh. A (Discovery Request); Exh. B (Gov't Response).

The devices are both material to preparing the defense and are expected to be used by the government at trial. Accordingly, the defense must be permitted to conduct its own inspection of the devices and should not be limited to only those items that the government's agent has selected as relevant to the government's case. To hold otherwise would lead to an absurd result. For example, imagine if the government seized a filing cabinet, searched it in its entirety, and sought to introduce one document from the cabinet at trial without giving the defense access to the filing cabinet. Or suppose the government produced only a couple of documents from a large binder and withheld the other documents from the defense. *United States v. Jeffers*, 570 F.3d 557, 571-72 (4th Cir. 2009) (finding Rule 16 violation where government refused to produce entire copy of government prepared binder and instead permitted the defense to copy only specific documents on a "case-by-case" basis). Or if the government produced just one side of a double-sided document. *See United States v. Lee*, 573 F.3d 155, 160-161 (3d Cir. 2009) (vacating conviction and granting new trial where government produced just one side of a two-sided document). But of course, and as the courts to pass on these questions have held, any of these illustrations would plainly result in a prejudicial discovery violation, That the items are digital devices does not change the

analysis. *See, e.g.*, *United States v. Halgat*, No. 2:13-CR-241-APG-VCF, 2014 WL 1612686, at *6 (D. Nev. Apr. 22, 2014), *rev'd on unrelated grounds*, 2016 WL 4528961 (D. Nev. Aug. 30, 2016) (compelling government to allow defense to conduct a forensic examination of undercover agent's phone).

The government faces a choice: it can either choose not to introduce any evidence from any of the digital devices, or it can make the devices available to the defense for inspection. The defense requests that the Court either compel the government to comply with its discovery obligations, or exclude all evidence from these devices in the government's case in chief at trial.

II. FACTUAL STATEMENT

A. The digital devices

Following the sinking of the *Conception*, the government seized several digital devices from different sources. These devices fall into three broad categories: 1) devices recovered from the wreckage belonging to the decedents or surviving employees of the boat; 2) devices seized during the execution of search warrants at the offices of Truth Aquatics, the owner of the vessel, and the other vessels owned by TA; and 3) miscellaneous devices seized from third parties who had relevant video or photographic evidence of the vessel either before or after the fire. Through this motion the defense requests that the Court require the government to elect whether to permit the defense to examine the digital devices falling under the first category or to exclude any evidence recovered from those devices at trial.[1]

1. Devices seized from the wreckage of the *Conception*

The *Conception* boat caught fire and sunk to the bottom of the ocean floor. After recovering the wreckage, the government sought an obtained a warrant to search the wreckage, including any digital devices recovered from it. Exh. C (Search Warrant

[1] A spreadsheet of all the devices recovered from the wreckage is included as Exhibit G.

Application and Warrant). The warrant outlined a search procedure for the digital devices. *Id*. ¶ 11. It required the search team to use "search protocols specifically chosen to identify only the specific items to be seized under this warrant."[2] *Id*. ¶ 11(b) (BOYLAN_00271479). The protocol allowed the search team to "subject all of the data contained in each digital device . . . to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized." The protocol also allowed the team to use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), and to search for and attempt to recover deleted, hidden, or encrypted data. *Id*. ¶¶ 11(b)(i), (iii) (BOYLAN_00271480).

The warranted permitted review of the electronic data by any government personnel assisting the investigation and authorized delivery of "a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review." *Id* ¶ 12 (BOYLAN_00271481-82).

The government separately obtained consent from some the decedents' next of kin to search the devices. The next of kin signed a consent form provided by the FBI, which said:

1. I have been asked by Special Agents of the Federal Bureau of Investigation to permit a complete search of: [device].
2. I have been advised of my right to refuse consent.
3. I give this permission voluntarily.
4. I authorize these agents to take any items, which they determine may be related to their investigation.

Exh. D (Redacted DOJ FBI Consent to Search Form).[3]

---

[2] No search protocols used on the digital devices recovered from the wreckage have been produced in discovery.

[3] Only one consent form is included because the other forms are virtually identical. This consent form was used to extract the contents of an iPhone, identified by the FBI as evidence number HQQ021386.

Dozens of digital devices were located during recovery efforts. All the devices sustained significant damage from the fire and/or were submerged in the ocean.

The recovered devices were turned over to the FBI. The Electronic Device Analysis Unit (EDAU) processed and triaged the devices. Exh. F. An electronics engineer tried to repair some of the devices, but did not succeed. Exh. F. However, approximately four of the devices were eventually able to be extracted after multiple separate attempts to repair them. *See, e.g.*, Exh. E. To extract the data from some of the devices, the device was connected to a forensic utility, and a "brute force" attack was initiated to recover the device PIN. *Id.* The device was unlocked using the recovered PIN, and then was connected to another forensic utility. The device was then extracted and a copy of the device was saved on a Blue-ray disc.

After obtaining the extraction, the case agent reviewed the content and tagged items he believed were relevant to the government's case. He then generated a report of only the tagged items. The report and the files that he tagged were produced to the defense in discovery. But the original extraction of the device, along with the device itself, remain in the custody, possession, and control of the FBI, and the government has declined several requests from the defense to review the extraction or conduct an independent examination of the device.

III. ARGUMENT

Rule 16(a) "grants criminal defendants a broad right to discovery." *United States v. Stever*, 603 F.3d 747, 752 (9th Cir. 2010). Federal Rule of Criminal Procedure 16(a)(1)(E) requires the Government to permit the defendant to inspect and copy objects within the government's possession, custody, or control if the item is "material to preparing the defense" or "the government intends to use the item in its case-in-chief at trial." Rule 16 "was adopted 'in the view that broad discovery contributes to the fair administration of criminal justice.'" *United States v. Johnson*, No. 14-CR-00412-TRH, 2015 WL 3630952, at *1 (N.D. Cal. May 6, 2015) (quoting advisory committee notes).

The defense believes that all the devices remain in the government's possession, custody, or control, so the question is whether they are material to preparing the defense *or* intended to be used by the government at trial. Both are true.

A. Inspecting the devices is material to preparing the defense.

For discovery purposes, "[m]ateriality is a 'low threshold.'" *United States v. Soto–Zuniga*, 837 F.3d 992, 1003 (9th Cir. 2016). "Rule 16 is thus broader than *Brady*. Information that is not exculpatory or impeaching may still be relevant to developing a possible defense. Even inculpatory evidence may be relevant." *United States v. Muniz-Jaquez*, 718 F.3d 1180, 1183 (9th Cir. 2013) (internal quotations and citations omitted). "The test is not whether the discovery is admissible at trial, but whether the discovery may assist [the defendant] in formulating a defense, including leading to admissible evidence." *Soto-Zuniga*, 837 F.3d at 1003. Indeed, "[i]nformation is material even if it simply causes a defendant to 'completely abandon' a planned defense and 'take an entirely different path.'" *United States v. Hernandez Meza*, 720 F.3d 760, 768 (9th Cir. 2013) (quoting *United States v. Doe*, 705 F.3d 1134, 1151 (9th Cir.2013)). A defendant demonstrates materiality merely by presenting facts that "tend to show" the requested materials are "helpful to the defense." *Muniz-Jaquez*, 718 F.3d at 1183 (quoting *Stever*, 603 F.3d at 752). Nothing more is required:

> A defendant need not spell out his theory of the case in order to obtain discovery. Nor is the government entitled to know in advance specifically what the defense is going to be. The relevant subsection of Rule 16 is written in categorical terms: Upon defendant's request, the government must disclose any documents or other objects within its possession, custody or control that are "material to preparing the defense."

Hernandez-Meza, 720 F.3d at 768.

At the same time, the burden on the government is heavy: "Lack of knowledge or even a showing of due diligence won't excuse non-compliance." *Hernandez-Meza*, 720 F.3d at 768. As the Ninth Circuit admonished, "[i]t thus behooves the government

to interpret the disclosure requirement broadly and turn over whatever evidence it has pertaining to the case." *Id*.

The Constitution imposes an independent duty on the government to turn over evidence favorable to a defendant. *Brady v. Maryland*, 373 U.S. 83, 87 (1963). "[T]he government violates its constitutional duty to disclose material exculpatory evidence where (1) the evidence in question is favorable to the accused in that it is exculpatory or impeachment evidence, (2) the government willfully or inadvertently suppresses this evidence, and (3) prejudice ensues from the suppression (i.e., the evidence is 'material')." *Silva v. Brown*, 416 F.3d 980, 985 (9th Cir. 2005) (citing *Strickler v. Green*, 527 U.S. 263, 281–82 (1999)). "When the 'reliability of a given witness may well be determinative of guilt or innocence,' nondisclosure of evidence affecting credibility falls within" the rule of *Brady*. *Giglio v. United States*, 405 U.S. 150, 154 (1972) (quoting *Napue v. Illinois*, 360 U.S. 264, 269 (1959)). Prosecutors have "a duty to learn of any favorable evidence known to the others acting on the government's behalf" and disclose it to the defendant. *Kyles v. Whitley*, 514 U.S. 419, 437-38 (1995).

An "inspection" under Rule 16 includes a forensic examination. Courts routinely permit defendants to forensically examine tangible objects under Rule 16. Wright & Miller, 2 Fed. Prac. & Proc. Crim. § 254 (4th ed. 2022); *United States v. Noel*, 708 F. Supp. 177 (W.D.Tenn.1989) (permitting the defendant to independently test a sample of an alleged controlled substance). Digital devices are no different. Rule 16 not only permits the defense to inspect but also to copy. *See United States v. Jeffers*, 570 F.3d 557, 571-72 (4th Cir. 2009) (finding Rule 16 violation where government refused to produce entire copy of government prepared binder and instead permitted the defense to copy only specific documents on a "case-by-case" basis). Thus, inspection necessarily includes obtaining a digital download of the device to conduct a forensic examination. *Halgat*, No. 2:13-CR-241-APG-VCF, 2014 WL 1612686, at *6 ("No logical leap is required to conclude that 'inspection' may include a forensic examination.").

Here, materiality is established because the government has identified files from the devices it seeks to introduce in its case-in-chief. *See United States v. Wolfson*, 294 F. Supp. 267, 277 (D. Del. 1968) ("If the documents seized or obtained by process from others are necessary to prove the Government's case at trial they would obviously be material to the preparation of the defense.").

Submitted *in camera* for the Court's review is a further explanation of materiality. *United States v. Hernandez-Meza*, 720 F.3d 760, 768-69 (9th Cir. 2013) ("A defendant needn't spell out his theory of the case in order to obtain discovery. Nor is the government entitled to know in advance specifically what the defense is going to be.").

B. Because the government intends to introduce evidence from the devices at trial, it must permit the defense to examine them.

The government intends to introduce evidence it obtained during its forensic search of the digital devices. Testimony about the devices and how they were searched is necessary to lay a foundation for the admissibility of the evidence obtained from those searches. That will include testimony about, for example, the government's repairs to the devices and the Cellebrite program used to forensically examine the devices. It is also anticipated that the government will elicit testimony about the metadata of the files it will introduce in its case-in-chief.

"A party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately." *United States v. Liebert*, 519 F.2d 542, 547-48 (3d Cir. 1975); *see also United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir.1970) ("It is quite incomprehensible that the prosecution should tender a witness to state the results of a

computer's operations without having the program available for defense scrutiny and use on cross-examination if desired.").[4]

The files that the government seeks to introduce at trial were extracted from the devices themselves. Without inspecting the device itself, the defense is unable to: (1) authenticate/validate the files the government produced; (2) analyze the seized item properly for defense strategy purposes; (3) determine how an artifact was utilized by the user; (4) verify the findings of government witnesses about electronically stored information; and (5) verify or dispute the veracity of claims by witnesses pertaining to the digital evidence.

What can be uncovered during a complete analysis of a forensic device is explained by Special Agent Jamie E. Wray in the declaration he submitted in support of the search warrant for the devices seized from the wreckage. In Paragraph 34 he declares that the following electronic evidence is often retrievable from digital devices:

> a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.
>
> b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

---

[4] Both out-of-circuit cases were cited with approval by the Ninth Circuit in *United States v. Budziak*, 697 F.3d 1105, 1112 (9th Cir. 2012).

> c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

But this evidence has not been made available to the defense. While no search protocols have been produced with respect to the agent's searches of the digital devices seized from the wreckage, the agent appears to have used Cellebrite to simply bookmark files falling within the date range of the diving trip.[5] But because the government intends to introduce those files and testimony about them in its case-in-chief, it must permit the defense to conduct its own examination to determine whether the government's examination was done accurately and completely.

In the alternative, if the government does not wish to make the devices available for inspection, it should be precluded from introducing any files from the devices at trial.

C. The Court has discretion to order broader discovery than Rule 16 prescribes.

Rule 16 "is intended to prescribe the minimum amount of discovery to which the parties are entitled. It is not intended to limit the [court]'s discretion to order broader discovery in appropriate cases." Advisory Committee Note, 1975 amendments. Courts have taken this seriously, holding that the rule does not limit their "inherent power" to order discovery that goes beyond what the rule authorizes. *See, e.g.*, *United States v. Lewis*, 511 F.2d 798, 803 n.8 (D.C. Cir. 1975). Even if the Court determines that Rule 16's minimum amount of discovery does not compel inspection of the digital devices, the Court should exercise its discretion to order an inspection in this case.

---

[5] Again, the government has not produced any search protocols used for searching the devices.

D. The government's arguments against inspection are unpersuasive.

The government has refused to comply with the defense's discovery request on primarily two grounds. First, as for the digital devices obtained by the government by the consent of a decedent's family member, the government asserts that allowing the defense to inspect and copy these items would raise privacy concerns and "dissuad[e] victims or their families from consenting to a limited search in the first place." Exh. B (March 9, 2023 Letter from AUSA Williams). But the government does not appear to have conducted a "limited search" of the decedents' devices, nor did family members limit their consent as such. Instead, the government seized the devices and created complete forensic images of them (which are still in its possession), pursuant to signed consent forms authorizing the government "to permit a *complete* search of" the devices. *See* Exh. D. (emphasis added). If the government is concerned about the decedents' privacy, the defense is amenable to entering into a protective order about this data. But the government cannot limit its production to self-selected data without permitting the defense to inspect the devices themselves. *See United States v. Halgat*, Case No. 2:13-cr-241-APG-VCF, 2014 WL 1612686, at *5-*6.

Privacy interests of third parties are outweighed by a defendant's Constitutional rights to a fair trial, due process, and access to exculpatory information. And several rules authorize disclosure of otherwise sensitive data if a defendant requires access to it in his criminal case. *See, e.g.*, Federal Rule of Criminal Procedure 17(c)(3) (permitting a subpoena for the production of personal or confidential information about a victim with a court order). In fact, defendants are allowed to inspect devices containing child pornography to prepare for a criminal trial. Here, the devices the defense seeks to inspect contain no contraband, but contain information that is material to the defense. It would make no sense to deny the defense access to these devices on privacy grounds, especially when a protective order can be entered.

Second, as to the defense's request to inspect and copy the digital devices obtained by the government through search warrants, the government argues that such a

request "would turn the well-established process, and Rule 41 itself, on its head." Ex. B (Williams Letter). But the purpose of Rule 41 is to protect against illegal searches and seizures by *the government*, and does not bind the conduct of the defense team. *Cf. United States v. Calandra*, 414 U.S. 338, 347 (1974) ("The purpose of the exclusionary rule is not to redress the injury to the privacy of the search victim . . . Instead, the rule's prime purpose is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures."). In any event, permitting the defense to inspect and copy the forensic copies of the digital devices already in the government's possession would not exceed the authority granted under the Rule 41 search warrants. The government's contention that it has only seized a limited set of responsive data from the devices is not accurate — they seized forensic images of the entire contents of the devices, and have analyzed those data sets and extracted items that its own agents deem relevant to the case. *See supra* II.B. But the agents cannot make such a relevancy determination on behalf of the defense. The complete forensic images remain in the government's possession, and fall squarely within the government's Rule 16 discovery obligations. *See Halgat*, 2014 WL 1612686, at *5-*6.

IV. CONCLUSION

For all these reasons, Mr. Boylan requests that the Court require the government to elect whether to permit the defense to examine the digital devices recovered from the *Conception* wreckage or to exclude any evidence recovered from the devices at trial.

Respectfully submitted,

CUAUHTEMOC ORTEGA
Federal Public Defender

DATED: March 23, 2023

By */s/ Georgina Wakefield*
GEORGINA WAKEFIELD
GABRIELA RIVERA
JULIA DEIXLER
Deputy Federal Public Defenders